International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Emotion Aware Multimedia Security using Role Base Access Control in Public Cloud Environment

Vaishali Uday Gaderao and Dr. Sunil D.Rathod

Department of Computer Engineering, Dr. D. Y. Patil School of Engg, Pune, India

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

The development of 5G Innovation has driven the wireless world into not needing obstacles to interconnect. The new technology aims to accomplish several challenging tasks and is designed to provide resource-intensive mobile terminals with more immersive and personalized services. The new 5 G network cloud computing has the ability to overcome this hurdle, allowing resource-intensive connectivity for mobile users through storage enabled by the mobile cloud and large data processing and distribution. In this research, a new platform named EMC in 5 G networks provides emotion-conscious, human-centric services via mobile cloud computing and affective services It is proposed that computation be. With the proposed design, the existing MCC architecture is revised to achieve the necessary Quality of Experience (QoE) in emotion-aware applications. Nevertheless, it brings with it a big challenge to securely obtain enough data to adequately protect the privacy of emotional data for emotional analysis. Tackling the security question, In this paper we propose emotion aware base user behavior in multi cloud environment, this system basically carried out deploy cloud platform with various user platforms where end user can communicate with cloud edge hand perform the transactional activities. The intermediate services can recognize the user behavior according to browsing history and identify the user's perspective using given machine learning base role based access disease. Implementation of system has done with Aamazon EC2 cloud environment, define the partial results which provides accepted accuracy than classical systems.

Keywords: *Security analysis, Access control, Emotion interaction, identity authentication, social robot*

Introduction

Multi-cloud storage Provides a solution to the risks and challenges of cloud computing by storing data via various cloud service providers (CSPs), including vendor lock-in, and data privacy. CSB is a Software-as -a-Service (SaaS) third-party cloud storage service provider that manages the relationship between one or more CSPs and cloud clients. Cloud is an emerging technology and cloud-based storage is a new concept that allows users not only to upload data to the internet, but also to easily access available resources and share data with anyone at any time. But cloud is a technique that generates a restore feature that enables clients to go back to a previous one attack state or Computer catastrophe provides an easy way to remove malware and computer security. The attackers have short-term windows where they should be trained and targeted for remote start-up and stoppage of VM. This is an extremely effective tool for defense. Because the hypervisor operates from Virtual Machine it is possible to control malware. VM Infrastructure will secure itself as a physical server infrastructure for such purposes.

2 Litarature Survey

Author Soni, Kritika, and Suresh Kumar et.al[1] Cloud computing provides easy access to shared computer resources (networks, servers, storage, applications and services) on demand. Models of data access control and comparison of their features. Comparison of the characteristics of all these models of security. Operation of role-based access and models based on access control attributes. RBAC has three different user elements, function and authorization. RBAC offers access to resources based on the functions permission. It simplifies the authorization process because many users may be given the same permission to perform the same role. According to Yang, Kan [2] Efficient, revocable data access control scheme for multiauthority cloud storage systems where multiple authorities coexist, and attributes can be given separately by each authority. They are specifically suggesting a multi-authority revocable CP-ABE scheme and using it to develop the data access control scheme as the underlying techniques. Our system of revocation of attributes will achieve protection both forward and backward.

Reddy, G. Venkatakoti [3] Multi-Authority Cloud Storage System with Users (DACMACS) Data Access Control and an appropriate and covered information curve for decoding as well. Therefore, setting up a modern multi-authorization Cipher text-policy attribute-based encryption scheme personally also design an appropriate method of canceling attributes to handle one and the other secured along with that low price also measured them time.

Rajput, Amitesh Singh et.al [4] carried out encrypted operations for the domain color correction were conducted over the cloud. As a result, it provides superior results, along with full assurance of privacy. Additionally, we'd be suggesting a block-based image encryption method using the logistic-tent scheme and the ElGamal cryptosystem. As a consequence the size of the encrypted image is significantly reduced compared with the naive approach. Photos taken from camera sensors to monitor the vision system for humans / machines are processed at their best.

Zhang, Yin, et al. [5] A security policy based Identity-based authentication and access control policy ensuring an integrated robot or edge system security certificate while retaining proper access control over the private data stored in the edge cloud; in particular, it adopts a polynomial-based approach control strategy and proposes a safe and effective access control scheme. This paper also introduces the identity authentication method for edge cloud systems, which can reduce overhead computation and authentication latency in a shared multi-edge cloud authentication. The Emotional computer, edge cloud, and remote cloud also store plenty of user-interacted personal data. Accordingly, the authorization to validate access to data is essential for user privacy protection. Several studies exist on access control and identity protection of a new type of network architecture, such as software-identified networks or cyber-physical systems (CPS).

According to Apolinário et.al [6] S-AUDIT, A platform that provides quality control of the data stored in business clouds. S-AUDIT uses homomorphic, digital signature authentication to prevent secure cloud access to data. To demonstrate how it can be used in real life, the software was combined with a cloud-backed file system called SCFS. Commercial cloud storage services like the Dropbox, Google Documents, Microsoft One Drive and Amazon S3 are widely accepted. Digital signatures are used for collective storage when data is exchanged between multiple cloud users and data is used by one single cloud user, MACs (Message Authentication Codes) are used for private storage.

Author Hussein, Nehad H. [7]. The cloud-based Safe storage and medical image sharing system recommended. The suggested solution is based on the number of cryptography techniques needed to create better protection over the transmission path and on the cloud for medical images. The following algorithms can be used here: Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), and Safe Hash (SHA-3). Once they are processed in the cloud, the third-party auditor is used to check the validity and reliability of medical images to reduce the computing burden on the computers of the clients. It also generates a digital signature to ensure the data source is secure and the robustness of the proposed Any leak or modification of data by scheme. The results show that the algorithm verifies data protection at a high level by encryption analysis.

Jeong, Junho, et al. [8] A secure IoT-based cloud Storage technology focused on a validated data-possession model, using Bloom filters. The experimental results showed that the proposed method saves time and has no significant differences with existing methods in the verification rate although the Bloom filter results in false positives. IoT technology allows a variety of devices to access the Internet, such as small sensors in a network.

Cui, Bo, Zhikun Lan et.al [9] Improved RBAC type called ET-RBAC. ET-RBAC incorporates environment module and time module constraints according to the original RBAC model in order to accomplish complex authorization and resource allocation of tasks. The non-relevant revocation approach is practiced for resource revocation and approvals to minimize the effect of dynamic changes on next-level task permits at the top-level feature.

We design and implement the ET-RBAC model including feature design, user design, authorization design, family group design, resource allocation process design. system.

Sukmana, Muhammad IH, et al. [10] MultiCSP Access Control Management Integrated Cloud Access Control Framework for Centralized and Automated User Services and Abstraction. Our proposal offers roles-based access control for CSB stakeholders to access cloud resources by assigning the necessary privileges and access control list to cloud resources and CSB stakeholders, respectively, in compliance with the privilege separation and the least privilege principle. We integrate our unified model into a CSB system called Cloud RAID for Business (CfB) with a network and cloud security service evaluation result for cfB and centralized management of resource and access control in multiple CSPs.

3 Proposed system details

3.1 Problem statement

In the proposed research work, we have designed and implemented a system that will provide data protection against aggression attacks in a reliable and unreliable cloud environment. The system will focus long communication scenario between data owner, user and authorities using different security techniques, it will provide highest security than all existing approaches.

3.2 Objective

- Provide the better security to all the data into the cloud system with emotional aware detection using deep learning.
- Implement a new verification as well as authentication protocol between authorities.
- Provide highest security from any type external or internal attack like collusion attack, SQL injection attack etc.

3.3 System Architecture

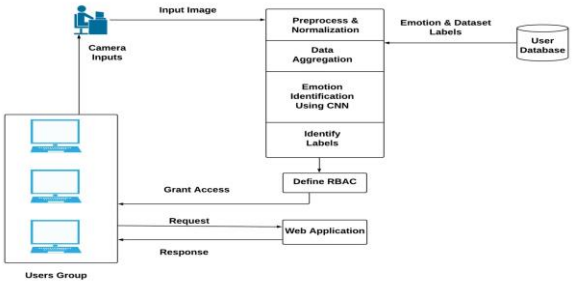

Figure 1: Proposed System architecture

3.4 Algorithm Design

Input : Training Rules Tr[], Test Instances Ts[], Threshold T.
Output : Weight w=0.0
Step 1 : Read each test instance from (TsInstnace from Ts)
Step 2 : $\text{TsIns} = \sum_{k=0}^{n} \{Ak \dots \text{An}\}$
Step 3 : Read each train instance from (TrInstnace from Tr)
Step 4 : $TrIns = \sum_{j=0}^{n} \{\text{Aj} \dots \dots \text{Am}\}$
Step 5 : ***w =*** *WeightCalc(TsIns, TrIns)*
Step 6 : if (w >= T)
Step 7 : Forward feed layer to input layer for feedback FeedLayer[] □ {Tsf,w}
Step 8 : optimized feed layer weight, Cweigt □ FeedLayer[0]
Step 9 : Return Cweight

3.5 Mathematical Model

The proposed system has define in cloud environment which is basically work end user and cloud web server.
Usre_Group= {UiD[1], UiD[2]….. UiD[n]} those user will communicate with our cloud system.
Web_Page ={Wp1, Wp2…..Wpn} This is the set of web pages.
Data-Owner[i] ={File[i]……n} data owner can upload the various files and set the credentials to end user.

File[i] □ {Access, Read, write, update, delete} □ {UiD[1], UiD[2]….. UiD[n]}
User can access the file using below formula from cloud

$$f(x) = U_i \leftarrow \sum_{n=1}^{\infty} (File[i])$$

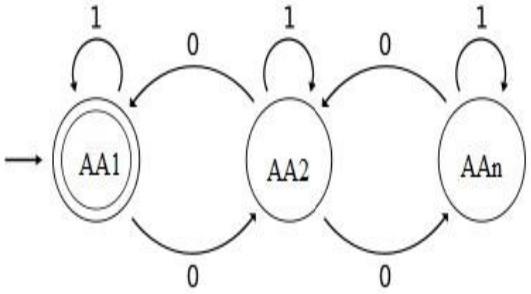

Fig 2 : State for each authority verification

Any t(n) return 1 then it will provide the private key otherwise state has change to another authority. $M = (Q, \Sigma, \delta, q_0, F)$ where
$Q = \{S_1, S_2\}$,
$\Sigma = \{0, 1\}$, $q_0 = S_1$,
$F = \{S_1\}$, and
The proposed state diagram shows the how users request processed by middle ware authority. When request has generated from end user it first receives by AA. If the AA1 is already acquired by some other process or busy then it will forward to another AA. This process works like recursively or base on round robin approach, when any t authority gets free it will return the keys to authenticated user.

Success Condition
$f(x)! = null$
or UiD[i] = Sucess Autheticate

Failure Condition
$f(x) == null$
$or\ Web_{page}\ Not\ found\ 404\ error$

4 Results and discussion

For the Evaluation of performance of the processes, accurate measurement of matrices. The software is designed with INTEL 2.8 GHz i3 processor on java 3-tier architecture platform and 4 GB of RAM on Amazon EC2 public cloud consol. We develop 2 physical network devices with Wi-Fi, and 10 VM with Amazon EC2 as a public cloud platform for system assessment. After some part of the system was implemented we got system performance at a reasonable level. Table 1 below shows the results of the proposed Elagamal algorithm for plain text conversion and encryption decryption.

Table 1: System performance (Estimated)

Data Size in MB	Encryption time (Milliseconds)		Decryption time (Milliseconds)	
	Existing	Proposed	Existing	Proposed
5	595	515	724	612
10	1120	1026	1132	1033
15	1680	1547	1687	1556
20	2260	2064	2231	2033

In The second experimental method illustrates the user's test time using various approaches. In the current system we find four specific authorities to be runtime verification. Below is the Fig. 3 Displays metrics of the output using different parameters with existing ones approaches.

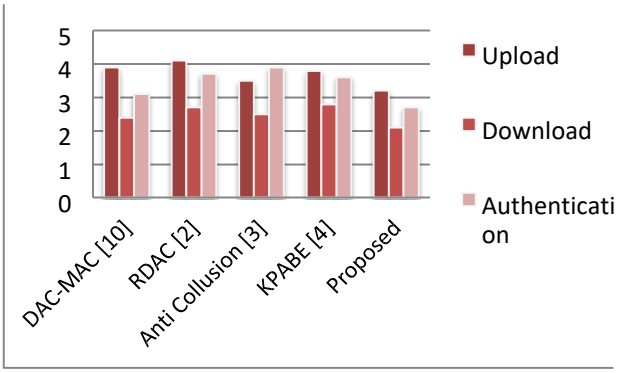

Fig. 3 : Evaluation of proposed system with various existing systems

Conclusions

This work Presents an identity authentication and access control approach for emotionconscious robot systems, and by analyzing their architecture, summarizes security concerns. This paper proposes a privacy protection of identity information with low overhead computation that supports edge cloud node mutual authentication, while a universal access control system fulfills the security requirement and supports a single user's edge cloud node and multiple devices. The efficacy of the authentication system for collective identity is higher than that of traditional approaches by research on the actual tested.

Future Works

To evaluate the proposed system on various distributed environment in fog nodes with different input objects.

References

[1]. Soni, Kritika, and Suresh Kumar. "Comparison of RBAC and ABAC Security Models for Private Cloud." 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon). IEEE, 2019.
[2]. Yang, Kan, and Xiaohua Jia. "Expressive, efficient, and revocable data access control for multi-authority cloud storage." IEEE transactions on parallel and distributed systems 25.7 (2014): 1735-1744
[3]. Reddy, G. Venkatakoti, B. Thirumala Rao, and Naresh Vurukonda. "A review on active data access control for multi-authority cloud storage systems with users." 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC). IEEE, 2017.
[4]. Rajput, Amitesh Singh, and
[5]. Balasubramanian Raman. "Privacy-Preserving Smart Surveillance Using Local Color Correction and Optimized ElGamal Cryptosystem over Cloud." 2019 IEEE 12th International Conference on Cloud Computing (CLOUD). IEEE, 2019.
[6]. Zhang, Yin, et al. "Emotion-aware multimedia systems security." IEEE
[7]. Transactions on Multimedia 21.3 (2018): 617624.
[8]. Apolinário, Filipe, Miguel Pardal, and Miguel Correia. "S-Audit: Efficient Data Integrity Verification for Cloud Storage." 2018
[9]. 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018.
[10]. Hussein, Nehad H. "Cloud-Based Efficient and Secure Scheme for Medical Images Storage and Sharing using ECC and SHA-3." 2019 2nd Scientific Conference of Computer Sciences (SCCS). IEEE, 2019.
[11]. Jeong, Junho, et al. "Secure Cloud Storage Service Using Bloom Filters for the Internet of Things." IEEE Access 7 (2019): 60897-60907.
[12]. Cui, Bo, Zhikun Lan, and Xiangyu Bai.
[13]. "Research on Role-based Access Control in IPv6 Smart Home." 2019 IEEE 9th
[14]. International Conference on Electronics Information and Emergency Communication (ICEIEC). IEEE, 2019.
[15]. Sukmana, Muhammad IH, et al. "Unified Cloud Access Control Model for Cloud Storage Broker." 2019 International Conference on Information Networking (ICOIN). IEEE, 2019.